Volume 18, Issue 31   Atari Online News, Etc.   August 5, 2016

Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1831   08/05/16

~ Hack Apple for Reward! ~ Windows 10 Anniversary ~ Firefox Is Updated!

-* PS4 and Xbox Superpowers Hub *-
-* Saturn Copy Protection Is Cracked! *-
-* Hillary Clinton’s Campaign Was Also Hacked *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Well, here we are, on the eve of another Summer Olympics. Just try to imagine all of these countries from all over the globe joining together to participate in many Olympic sporting events - in peace. What a novel idea. And, like past Olympic Games, many ponder why the world can’t act in typical harmony? The novel idea really boggles the mind! While Brazil faces current political problems, it appears that the country has come together to host the Games. I look forward to watching numerous events throughout the upcoming days (as the opening ceremonies play in the background as I put the finishing touches on this week’s issue).

Until next time...

=~=~=~=

->In This Week’s Gaming Section - This USB Hub Gives Your PS4 and Xbox Superpowers!
"""""""""""""""""""""""""""""   Saturn’s Copy Protection Finally Cracked!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

This USB Hub Gives Your PS4 and Xbox Superpowers

In the bitter war between console and PC gamers, there is one statement neither side can find contentious. It doesn t matter how much you adore your PS4 or your Xbox One or your Atari Jaguar, consoles suck when playing first person shooters. Man was not meant to frag one s enemies using two joysticks and some trigger buttons. The beauty of the Xim4 USB hub is that it lets you destroy shit-talking tweens as God intended: with a keyboard and mouse.

That s not something console game designers are crazy about. Currently, both major consoles can accept keyboard and mouse input, but the designers of games like Destiny and Overwatch have purposely deactivated those inputs to keep precision mouse fraggers from having a significant advantage over their clumsy thumbed controller brethren. I m one of those clumsy-thumbed sons of bitches. So after getting repeatedly boned one weekend in Overwatch, I started reading up on ways to up my game. Reddit was full of people swearing by the Xim4 or claiming console pros swear by it.

Every top ranked PS4 user uses it, one redditor insisted.

I couldn t confirm that claim, but I thought trying the Xim4 out was a nice alternative. Maybe it would improve my game and give me an edge that would take me from completely ordinary to slightly above average. The Xim4 uses witchcraft and technological wizardy to get around the blocks put in place by game manufacturers and makes Overwatch (or other FPS) on the PS4 virtually identical to Overwatch (or other FPS) on the PC.

But the road to success isn t as simple as plugging and playing. The $125 Xim4 is technically a hack, and that means you have to spend a little time setting it up before you can do sweet quick turns and middle mouse clicks for punching. First, you have to make sure the mouse and keyboard you have will work with the Xim4 by double checking its website. Then, you have to do the same for the games you plan on playing.

Once you re sure everything checks out and have spent you $125, you plug both into the hub, then you plug the controller into the hub, and then plug the hub into the console. The Xim4 is essentially hijacking the controller s signal, so inputs from your mouse and keyboard will appear to be from the controller instead neatly getting around developers blocks on keyboards and mice.

But you still need to be able to tweak the settings, choose the games you want the Xim4 to work with, and bind all your keys to buttons on the controller. You do that via the Xim4 Manager, which is available for PC, Mac, Android, and iOS devices.

The Xim4 manager is an ugly hack looking piece of software, but it has the ability to save profiles, so you can make one for every character on Overwatch or every class on Battlefield 4. Setting up each profile takes time. It s not easy. If you are planning to grab a Xim4 and get to playing games in under thirty minutes you re probably out of luck. The set up and keybinding process can taken anywhere from a minute to ten minutes, and after that you have to tweak   a lot.

Mouse settings are especially complex. See, controller joysticks lack precision which is why so many top gamers prefer using a mouse. But console game developers try to get around the terrible precision by introducing something called aim assistance. It s supposed to help you nudge the reticle on screen towards the alien you want to explode, by anticipating your movements and doing it for you.

It s great in theory, but it s imprecise and can be clumsy in practice   particularly if you re actually really good at aiming. Add a mouse to the experience, and your reticle positioning can get... whacky. It will jerk all over the screen or move so slow you ll wonder if the console is freezing. So you have to tweak the settings a lot, and if your mouse is one of those super fancy ones with onboard memory then you have to go even further. This means tweaking the mouse s settings on your computer, and then tweaking the settings on the console in the game of your choice.

The tangle of settings is one of the biggest hassles of the experience. Another headache is that fact that the Xim4 doesn t charge your controller while plugged in, which makes it a worthless hunk of plastic if your controller dies mid-game.

Once you re past the hurdles of hardware hacking the hell out of your console, the experience is sublime. Sure, I forget which button I have linked to which key and have to double check them periodically. And no, the Xim4 cannot do anything to miraculously fix my completely average aim.

But man, I felt like some sort of golden god while playing. I ve never used hacks in a multiplayer game before, but I suddenly understood the appeal. So many more of my shots were hitting just right. Quick reflex-focused playstyles that are virtually impossible to do on a controller were at my command, and even though I was terrible at those playstyles, I was still better than the other guy. Which is all that matters.

If you re in the weeds on your favorite first person shooter, or just want to experience the wonder that all those PC gamer nerds talk about, than do it my poor aiming sisters and brothers. Spend $125 on a Xim4. It might be the closest you ll ever get to superpowers.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

""""""""""""""""""""

Sega Saturn’s Copy Protection Finally Cracked, Giving Retro Gamers A New Option

Excessive wear, heat, and just plain old age can all wreak havoc on CD-based game consoles. The Sega Saturn, now more than two decades old, is at risk of becoming essentially extinct due to disc drives inside no longer being able to read games. But one dedicated wizard took it upon himself to crack the system s DRM, and preserve its library.

Dr. Abrasive (real names James Wah), who previously created Drag n Derp for easily loading files onto Game Boy cartridges via USB, was interested in developing software for the Sega Saturn next due to its multi-channel sound chip, but found that the console s copy protection system made it impossible.

 It actually works quite well. It detects the little wobble in the outer rim of the CD when it s trying to read the protection data, Wah says. And that s not something you can do with a CD burner.

Wah was able to acquire a Sega Saturn s CD module CPU, which he connected to a circuit board of his own and tricked into revealing the entirety of its ROM contents to him. He was then able to use this information to determine exactly how the console s operating system worked.

 There are bits [of code] that have been written by hand and edited several times, Wah says. I ve actually been really surprised by much you can see of its development history just by kind of looking at the code.

After examining a slot for a peripheral card on the back of the system, Wah opted to circumnavigate the CD drive altogether, instead using tentacles and a small card plugged into the peripheral slot to effectively replace the drive completely. He has now also implemented the ability to read and write files directly to a USB drive while the system is running, which allows you to store saved game files.

Curiously, though the Sega Saturn has remarkable copy protection on the system itself, the discs can be read on a PC without issue. This allows anyone to easily load them onto a USB stick for use in the cracked console.

 These consoles, the CD drives are slowly dying. And especially in the west, it was never that popular a console that generation. So finding spare parts is actually a little bit difficult, Wah says. Ultimately I d like to help homebrew become accessible and also more powerful with a USB interface, but I d like to see it with a place in archiving.

For more information about the challenges Wah still faces and footage of the cracked system in action, check out the video at the top of the page.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Hillary Clinton’s Presidential Campaign
Also Hacked in Attack on Democratic Party

The Associated Press confirmed yesterday that the computer systems used by Hillary Clinton’s presidential campaign were hacked as part of the recent Democratic National Convention (DNC) hack.

Last week’s email dump containing almost 20,000 emails from top DNC officials was just the beginning, which led DNC Chairwoman Debbie Wasserman Schultz to resign as the group s leader, as WikiLeaks announced that it was part one of its new Hillary Leaks series.

This suggests WikiLeaks Founder Julian Assange has had his hands on more data from the DNC hack that, according to him, could eventually result in the arrest of Hillary Clinton.

In an interview with Robert Preston of ITV last month, Assange made it clear that he hopes to harm Hillary Clinton s chances from becoming president of the United States, opposing her candidacy on both policies as well as personal grounds.

Assange also stressed that he had "a lot more material" about Clinton’s presidential campaign that could possibly provide enough evidence for the indictment of Hillary Clinton.

Now, when it has been reported that the computer systems used by Clinton’s presidential campaign were breached as part of the DNC hack, one could guess this could be the next release in the Hillary Leaks series by Assange.

According to federal law enforcement officials and some cybersecurity experts, the DNC hack is believed to be an attempt by the Russian intelligence services to influence the presidential election.

U.S. intelligence agencies have reportedly concluded that the Russian government was behind the theft of the DNC emails and documents. Although, it’s unclear whether the attack was fairly routine espionage or an effort to manipulate the presidential election.

Even, security firm CrowdStrike, who first investigated the DNC hack, said that the group that hacked into the DNC servers in April 2016 was engaged in extensive political and economic espionage to benefit Russian government and closely linked to the Russia’s powerful and highly capable intelligence services.

According to the firm, the Fancy Bear APT (also known as APT28 and Pawn Storm) used a piece of malware called X-Tunnel to steal data from the system without getting detected.

Most recently, security firm Invincea also released its own report, saying X-Tunnel was used to steal the data from the DNC servers, but since the malware appeared to be a repurposed open source tool from a Chinese company, the firm did not support or refute "the Russian origins of the XTunnel binary."

The F.B.I. said in a statement that it "is aware of media reporting on cyber intrusions involving multiple political entities, and is working to determine the accuracy, nature, and scope of these matters."

We still have to accept the fact that someone is attacking America’s computer systems in an attempt to influence the presidential election.

So this kind of politically motivated attack can become even worse in November   at the time of voting.

Security expert Bruce Schneier stressed that since Clinton’s computer systems can be targeted as part of DNC attack, it is possible that America’s election systems and voting machines could also be vulnerable to a similar attack.

"We need to secure our election systems before autumn," says Schneier via the Washington Post. "If Putin’s government has already used a cyber attack to attempt to help Trump win, there’s no reason to believe he won’t do it again   especially now that Trump is inviting the "help.""

Since more and more states have moved to electronic voting machines and Internet voting over the past years, it has made a way for hackers to manipulate these systems.

Schneier suggests the government to "create tiger teams to test the machines and systems resistance to attack, drastically increase their cyber-defenses" and if can not guarantee their security online, take them offline.

If You Value Privacy, WikiLeaks Stopped Being Your Friend Years Ago

The Democratic Party can t be happy with WikiLeaks after that site published 19,252 emails taken from the Democratic National Committee s servers. But party donors should be even angrier.

WikiLeaks, perhaps best known for its 2010 disclosure of video showing US soldiers fatally shooting Iraqi civilians, on Friday posted a trove of messages to and from the DNC that included home addresses, Social Security numbers and other personally identifiable information found in routine donation records.

Some cybersecurity experts believe Russian operatives leaked the DNC emails to Wikileaks, which describes itself as a multi-national media organization and associated library.

And its Twitter account has been getting into the creepy zone lately. Should you take this group as the independent guardian it portrays itself to be? I m going to say no.

As Gizmodo and other news sites observed, if you search for Contribution in WikiLeaks s DNC archive, you ll see where these contributors live, the last four digits of some of their credit cards, and sometimes even their Social Security and passport numbers.

 There s no clear public-interest value in publishing them, said Alex Howard, a senior analyst with the Washington-based transparency group Sunlight Foundation. Instead, Howard says the act was ethically dubious if not outright reprehensible.

The DNC should have known to encrypt information that sensitive, and an organization as security-conscious as WikiLeaks should have known not to publish it. Yet its Twitter account said this large-scale unmasking of private citizens isn t an error.

An e-mail sent to WikiLeaks media-contact address Tuesday went unanswered.

Wikileaks DNC archive did reveal some concerning episodes. In one e-mail, a Politico reporter let a DNC staffer inspect an unpublished story. Others showed the DNC working behind the scenes to support Hillary Rodham Clinton s nomination.

(The Republican National Committee had its own ambitions to find and back an establishment candidate, but the RNC seems to have escaped WikiLeaks attention).

But exposing wrongdoing doesn t demand a data breach, and doxing isn t reporting. International Consortium of Investigative Journalists director Gerard Ryle recently summed up this sentiment to Wired after his organization published its carefully screened Panama Papers money-laundering report.

WikiLeaks has done this before. It exposed Afghan intelligence sources in 2010   founder Julian Assange said he was only obliged to protect those facing unjust retribution   and then revealed human-rights activists in a 2011 dump of State Department communications.

Separate research by security firms Fidelis, Mandiant and ThreatConnect strongly suggests WikiLeaks got these e-mails from Russian intelligence agencies who earlier hacked into the DNC. That makes today s site look even less like the one that helped document a secretly negotiated, multinational deal called the Anti-Counterfeiting Trade Agreement in the late 2000s.

Vladimir Putin may not be trying to influence the election, but Assange clearly loathes Clinton and has threatened to reveal more DNC details soon.

 The timing of the DNC leaks raises questions, wrote James Love, director of Knowledge Ecology International. If WikiLeaks is able to get Donald Trump elected, well, I think that will have consequences for everyone, and I don t see how Assange sees this as a positive.

Knowledge Ecology International relied on WikiLeaks documents for its criticism of ACTA and the Trans-Pacific Partnership trade agreement, and Love said earlier dealings with Assange s group had been pleasant: In the TPP leaks, they did a lot of work to protect the sources.

Assange, Howard said, has a history of seeing Western democracies as a bigger threat than the likes of Russia or China. He asked Assange about that during the WikiLeaks founder s video appearance at a conference in Mexico City, and, Howard recalled, He got fairly upset about it.

WikiLeaks recent Twitter output also suggests strange priorities. That account invited its 3 million-plus followers to browse a now-offline archive of e-mails from Turkish citizens, violating their privacy for no good reason, and even tweeted poorly veiled anti-semitic insults, which the organization has since deleted.

Electronic Frontier Foundation director for international freedom of expression Jillian York, a past WikiLeaks supporter, tweeted Thursday that she was done with the group: Support isn t unconditional and this week nailed that coffin.

Other civil-liberties groups still back WikiLeaks. The Freedom of the Press Foundation features a prominent fundraising link for WikiLeaks on its own homepage.

The outrage over WikiLeaks s carelessness with the info of innocents yields to the realization that other organizations have made comparable mistakes   even if they could point to legal reasons that argued for exposing people s personal information.

US police departments made arrest-record databases publicly searchable, then mugshot sites collected arrest photos and charged extortionate fees for maybe removing them. A suburban New York newspaper aimed to dramatize the extent of gun ownership in two counties by taking addresses of registered gun owners, available through a public-records search, and putting them on a searchable map. Washington s elections board read the law narrowly in deciding to post a searchable database of the names, home addresses and voting history of D.C. residents.

All of those actions publicized personal data that citizens could not have reasonably expected to become search-engine bait. How many other databases are waiting to go online through a hack or intentional sharing?

Something Assange said in a remote video appearance at the SXSW conference in 2014 comes to mind: It s not the case anymore that you can kind of hide from the state, that you can keep your head down. More of WikiLeaks latest help can only assure that.

The World’s Best Hackers Are Taking Over Vegas at DEF CON 24

On Thursday, a group of the world s brightest, most dangerous nerds will spend three days in the sweltering Las Vegas heat (well, inside of an air-conditioned ballroom at the Paris Hotel) to take part in the 24th annual DEF CON hacking conference.

You know all of those stories about hackers being able to trick subway turnstiles to get free rides or taking over cars diagnostic systems? Those all came from DEF CON.

So just what is DEF CON? Well, it s one of the largest and oldest hacking conventions in the world. It started in 1993 and has been held in Vegas every summer since.

And before you ask, no, everyone there isn t dressed in long black trench coats like Neo from The Matrix or whatever kind of weird Vulcan-surfer hybrid thing Angelina Jolie had going on in Hackers. These are academics, professionals, government officials, and yes, some really, really, really impressive hackers.

DEF CON isn t nearly as stuffy or formal as your average tech convention. It s actually, well, fun. The entire event is based around hackers and researchers giving talks on topics ranging from hacking hotel rooms to cats being used to help hack your neighbor s Wi-Fi network.

The show brings hackers together so they can hang out in real life, knock back a few drinks and trade information on their latest hacking accomplishments. It s also a place for hackers to test their abilities against their fellow attendees and the hapless Vegas vacationers who are completely unaware they re in the midst of thousands of accomplished hackers who can take over their phones, tablets and laptops with ease.

In fact, to prepare for attending DEF CON, it s a good idea to completely disconnect from the internet or any other wireless device. That means when you re on-site, you need to turn off your phone s Wi-Fi, cellular connection, Bluetooth and other radio that can send and receive signals.

Why? Because if you don t, your device will without a doubt be hacked. That s not some kind of hyperbolic warning meant to keep you safe, either. That s the absolute truth. I m heading there this week, and I m going to have a burner phone with me to ensure my real phone doesn t get hacked. And if I do get hacked, well, that ll make a pretty great story.

The vast majority of hackers don t attend DEF CON to hack into attendees devices and steal their information. They largely do it for the thrill and to simply know that they can.

This year s DEF CON coincides with DARPA s Cyber Grand Challenge event, where seven teams will compete to see if software they developed will be able to find and fix security vulnerabilities in a computer program. If successful, it would prove to be an incredible step forward in cyber security.

But don t expect the hackers at DEF CON to throw up their hands if the CGC results in self-protecting software. If anything, they ll welcome a new challenge.

So if you see me on Twitter next week posting tweets that seem to be more ridiculous than normal, I ve probably been hacked at DEF CON. I can t wait.

Hack Apple & Get Paid Up to $200,000 Bug Bounty Reward

So finally, Apple will pay you for your efforts of finding bugs in its products.

While major technology companies, including Microsoft, Facebook and Google, have launched bug bounty programs over last few years to reward researchers and hackers who report vulnerabilities in their products, Apple remained a holdout.

But, not now.

On Thursday, Apple announced at the Black Hat security conference that the company would be launching a bug bounty program starting this fall to pay outside security researchers and white hat hackers privately disclose security flaws in the company’s products.

How much is a vulnerability in Apple software worth? Any Guesses?

It’s up to $200,000.

Head of Apple security team, Ivan Krstic, said the company plans to offer rewards of up to $200,000 (£152,433) to researchers who report critical security vulnerabilities in certain Apple software.

While that’s certainly a sizable bounty reward   one of the highest rewards offered in corporate bug bounty programs.

Well, for now, Apple is intentionally keeping the scope of its bug bounty program small by launching the program as invitation-only that will be open only to limited security researchers who have previously made valuable bug disclosures to Apple.

The company will slowly expand the bug bounty program.

Launching in September, the program will offer bounties for a small range of iOS and iCloud flaws.

Here’s the full list of risk and reward:

Flaws in secure boot firmware components: Up to $200,000.

Flaws that could allow extraction of confidential data protected by the Secure Enclave: Up to $100,000.

Vulnerabilities that allow executions of malicious or arbitrary code with kernel privileges: Up to $50,000.

Flaws that grant unauthorized access to iCloud account data on Apple servers (remember celebrity photo leak?): Up to $50,000.

Access from a sandboxed process to user data outside of that sandbox: Up to $25,000.

For the eligibility of a reward, researchers will need to provide a proof-of-concept (POC) on the latest iOS and hardware with the clarity of the bug report, the novelty of the bounty problem and the possibility of user exposure, and the degree of user interaction necessary to exploit the flaw.

Earlier this year, Apple fought a much-publicized battle with the FBI over a court order to access the locked San Bernardino shooter’s iPhone.

When the FBI forced Apple to unlock the shooter’s iPhone, it refused, eventually making the bureau hire professional hackers to break into the iPhone - supposedly paying out over $1 Million.

Perhaps the company is trying to eliminate these lucrative backdoors into its software to make its iOS devices so secure that even the company can not crack them.

Apple Announces Invitation-only Bug Bounty Program at Black Hat Conference

An Apple security chief unexpectedly announced the company will pay for vulnerabilities found in certain aspects of iOS and iCloud. The program is invitation only, and payouts will be based on severity and category. The top fees across five areas range from $25,000 to $200,000, but could be much lower. The announcement came during a presentation by Ivan Krstic, Apple s head of security engineering and architecture, at the Black Hat security research conference in Las Vegas.

The presentation also included a level of technical detail and disclosure of security here, related to AutoUnlock, HomeKit, and iCloud Keychain that has been mostly absent in the past at conferences, according to those present.

The fees offered aren t enough to deter those merely in it for the cash, as major flaws can command cash from malicious and legitimate parties alike that far exceeds Apple s top rates. But it could help convince researchers to disclose problems to Apple and remain mute until the bugs are patched. In some instances in the last few years, those who had discovered exploits went public after they decided sufficient time had passed without Apple providing updates.

Most of Apple s competitors for customers and eyeballs already run so-called bug bounty programs, in which researchers or hackers turn over what they know in exchange for a fee, usually paid in cash, and keeping quiet until fixes ship. Some sponsor hacking events, paying out in cash, equipment, or both for achieving a goal, like breaking out of a browser sandbox designed to contain malicious software from the rest of a system. Amazon now remains the exception among large Internet firms.

Details were assembled from participant reports; the presentation isn t available online, and Apple hasn t posted details yet. We have a query out to Apple for more information; some researchers and publications were briefed under embargo ahead of time.

Krstic listed five categories of bugs and the top fee paid for each. Those who attended say that macOS isn t yet covered as part of the program.

Secure boot firmware components ($200,000 cap)

Extraction of confidential material protected by the Secure Enclave Processor ($100,000 cap)

Execution of arbitrary code with kernel privileges ($50,000 cap)

Unauthorized access to iCloud account data on Apple servers ($50,000 cap)

Access from a sandboxed process to user data outside of that sandbox ($25,000 cap)

Each of these aspects represents key vectors for attack by governments and criminals alike. While iOS has never had exploits spread significantly in the wild, jailbreaking software has made use of various methods of running arbitrary code. In a separate Black Hat presentation, the makers of the Pangu jailbreak for iOS 9 (fixed in 9.2) described how they achieved that kind of code execution.

So far, there s been no known extraction of data from Secure Enclave, the dedicated hardware in iOS devices with an A7 or newer process that acts as a one-way valve to store fingerprint characteristics and certain data associated with Apple Pay. It s also used to prevent downgrading iOS to exploit a bug in a previous release.

While iCloud accounts have been compromised in the past through certain weak password entry endpoints and social engineering of celebrity accounts, there s been no reported breach of iCloud servers.

Those invited to apply to the program will have to provide a proof of concept that works on current software and hardware. Bounties will be based on a combination of factors, as with other corporate bug programs, such as how much interaction is required from a user to trigger it, the exploit s severity, how novel it is compared to previously known issues, and how clearly the flaw is described.

Apple has also offered a bump to bug finders who want to donate their awards to charity. At its discretion potentially to avoid supporting charities at odds with its image or public stances Apple will match donated awards dollar for dollar.

Security researcher Rich Mogull, a contributor to Macworld and other Apple-focused publications, noted in a post on his company s blog that Apple will consider adding those who discover bugs but haven t been invited to the bounty program. Apple won t publish a list of invitees, he writes, but those participating are free to disclose it. Mogull writes a couple of dozen researchers have received initial invitations. This is clearly intended to reduce the volume of reports and keep the quality high. Apple has long accepted bug reports without the potential of compensation, and that continues.

Apple began to acknowledge researchers who conformed to its advance disclosure and testing rules several years ago and includes their name and company affiliation (if any) in security updates. Apple withholds credit and sometimes publishes those who work outside its guidelines, most prominently suspending Charlie Miller, who had previously discovered many flaws, from its developer program in 2011 after he had an app approved in the App Store with a proof-of-concept flaw embedded.

Bugs pay big on gray and black markets, with criminal syndicates and government agencies sometimes vying for the same exploit before it s found and patched. These so-called zero-day bugs, ones that aren t patched before they re used to exploit a weakness, allow malicious and legitimate parties alike ways to crack servers, operating systems, and sometimes individual computers and mobile devices. Effective cracks can go for tens of thousands of dollars, with reports putting the top rate at a million dollars.

The Department of Justice dropped its attempt to force Apple to create a specialized version of iOS that would allow the FBI to attempt to crack a work-provided iPhone used by San Bernardino mass-killer Syed Rizwan after it obtained a bypass from a third party.

Fees at other companies range from a starting point from $100 to $500, and are capped at from $20,000 at Google to $100,000 at Microsoft. Some companies don t have an announced cap, and may offer far higher fees for major exploits.

Hacker Selling 200 Million Yahoo Accounts on Dark Web

Hardly a day goes without headlines about any significant data breach. In the past few months, over 1 Billion account credentials from popular social network sites, including LinkedIn, Tumblr, MySpace and VK.com were exposed on the Internet.

Now, the same hacker who was responsible for selling data dumps for LinkedIn, MySpace, Tumblr and VK.com is now selling what is said to be the login information of 200 Million Yahoo! users on the Dark Web.

The hacker, who goes by the pseudonym "Peace" or "peace_of_mind," has uploaded 200 Million Yahoo! credentials up for sale on an underground marketplace called The Real Deal for 3 Bitcoins (US$1,824).

Yahoo! admitted the company was "aware" of the potential leak, but did not confirm the authenticity of the data.

The leaked database includes usernames, MD5-hashed passwords and date of births from 200 Million Yahoo! Users. In some cases, there is also the backup email addresses used for the account, country of origin, as well as the ZIP codes for United States users.

Since the passwords are MD5-encrypted, hackers could easily decrypt them using an MD5 decrypter available online, making Yahoo! users open to hackers.

In a brief description, Peace says the Yahoo! database "most likely" comes from 2012, the same year when Marissa Mayer became Yahoo’s CEO.

Just last week, Verizon acquired Yahoo! for $4.8 Billion. So, the hacker decided to monetize the stolen user accounts before the data lose its value.

When reached out, the company said in a statement:

"We are committed to protecting the security of our users' information and we take such claim very seriously. Our security team is working to determine the facts...we always encourage our users to create strong passwords, or give up passwords altogether by using Yahoo Account Key, and use different passwords for different platforms."

Although the company has not confirmed the breach, users are still advised to change their passwords (and keep a longer and stronger one using a good password manager) and enable two-factor authentication for online accounts immediately, especially if you are using the same password for multiple websites.

You can also adopt a good password manager that allows you to create complex passwords for different sites as well as remember them for you.

We have listed some best password managers here that could help you understand the importance of password manager and help you choose a suitable one, according to your requirement.

Torrentz.eu Shuts Down Forever!
End of Biggest Torrent Search Engine

Over two weeks after the shutdown of Kickass Torrents and arrest of its admin in Poland, the world's biggest BitTorrent meta-search engine Torrentz.eu has apparently shut down its operation.

The surprise shutdown of Torrentz marks the end of an era.

Torrentz.eu was a free, fast and powerful meta-search engine that hosted no torrents of its own, but combined results from dozens of other torrent search engine sites including The Pirate Bay, Kickass Torrents and ExtraTorrent.

The meta-search engine has announced "farewell" to its millions of torrent users without much fanfare, suddenly ceasing its operation and disabling its search functionality.

At the time of writing, the Torrentz.eu Web page is displaying a message that reads in the past tense:

"Torrentz was a free, fast and powerful meta-search engine combining results from dozens of search engines."

When try to run any search or click any link on the site, the search engine refuses to show any search result, instead displays a message that reads:

"Torrentz will always love you. Farewell."

Launched back in 2003, Torrentz has entertained the torrent community for more than 13 years with millions of visitors per day.

However, today, the popular meta-search engine has shut down its operation from all Torrentz domains, including the main .EU domain (both HTTP and HTTPS version) as well as other backups such as .ME, .CH, and .IN.

Although many copyright holders were not happy with the site with both RIAA and MPAA have reported the site to the U.S. Government in recent years, says TorrentFreak, there is no news of any arrest or legal takedown of the site in this case.

Still, it would be fair enough to wait for an official announcement from the site owners.

Bitcoin Price Drops 20% After $72 Million in Bitcoin Stolen from Bitfinex Exchange

Yet another blow to Bitcoin: One of the world’s most popular exchanges of the cryptocurrency has suffered a major hack, leading to a loss of around $72 Million worth of Bitcoins.

Hong Kong-based Bitcoin exchange ’Bitfinex’ has posted a note on their website announcing the shutdown of its operation after discovering a security breach that allowed an attacker to steal some user funds.

While the company did not mention a total amount lost in the breach, one of their employees   Bitfinex community director Zane Tackett   confirmed on Reddit that the total amount stolen was 119,756 bitcoins   worth up to $72 Million in cash.

The cause of the security breach and the hacker behind the incident is still unclear, but the attackers appear to have mysteriously bypassed Bitfinex s mandated limits on withdrawals.

"The theft is being reported to   and we are co-operating with   law enforcement," Bitfinex statement reads.

"We will look at various options to address customer losses later in the investigation" and "ask for the community s patience as we unravel the causes and consequences of this breach."

Bitfinex is the third-largest Bitcoin exchange in the world. After the news of the Bitfinex hack had broken on August 2, the price of Bitcoin dropped almost 20%, from $602.78 to $541 per Bitcoin, within the day after the announcement.

The sudden dropout could be the result of the latest hack that likely made Bitcoin investors sell off their Bitcoin holdings, leading to a rapid decrease in Bitcoin price.

Bitfinex’s security firm Bitgo   a Palo Alto-based Bitcoin security company that allows bitcoin exchanges to provide separate, multi-signature wallets for each user’s funds tweeted earlier today, saying it has not found any "evidence of a breach on any BitGo servers" during its investigation.

Although it s unclear whether Bitfinex can sustain a loss of that magnitude, the company will address any customer losses following the result of their ongoing investigation.

"As we account for individualized customer losses, we may need to settle open margin positions, associated financing, and/or collateral affected by the breach," the company says. "Any settlements will be at the current market prices as of 18:00 UTC."

The bottom line:

The best way to secure yourself is to go OFFLINE.

Facebook Is Changing Its News Feed Again,
And You ll Never Guess How!

Five Reasons You Should Care Facebook Is Changing Again

The Inside Scoop On The Latest Change To Facebook

You’ll Never Guess What Facebook Is Doing This Time!

So much for headlines like that. The world’s largest social network is going up against internet journalism’s biggest scourge: click bait.

You know what I’m talking about. They’re the type of headlines that overpromise and underdeliver, that lure you into reading something without substance.

In recent years, these headlines have followed a predictable format, written with drama and pizzazz but far less informative than The New York Post’s famous "Headless Body In Topless Bar."

If that were rewritten as click bait, it’d probably be: "You’ll Never Guess What They Found In THIS Bar!"

Facebook is weeding these headlines out by - no surprise - training an algorithm on the problem. The company has already identified and punished people who post click bait headlines by watching how much time lapses between someone clicking on a link and then returning back to Facebook. Too short, and it’s probably click bait.

Businesses can’t tweet #TeamUSA or #Rio2016 because reasons
The smartphone has become the center of our political lives
Facebook is training employees to avoid political bias

Now the company’s going even further.

Facebook categorized tens of thousands of headlines as click bait, then taught a computer to identify new, similarly useless examples.

Click bait headlines tend to be similar, the company said. They typically withhold information or exaggerate what the story is actually about.

A Facebook spokeswoman declined to say which publications the company had identified as the worst offenders, though I’ve got my eye on a few. None of them apparently has been warned about this change.

"We anticipate that most Pages won’t see any significant changes to their distribution in News Feed as a result of this change," Facebook data scientist Alex Peysakhovich and company researcher Kristin Hendrix said in a statement. "Websites and Pages who rely on click-bait-style headlines should expect their distribution to decrease."

We’ll see. Or should I say: You Wouldn’t Believe What’s About To Happen To Click Bait Headlines!

Microsoft Wields Windows 10 Notifications Against Chrome Browser

Microsoft is keeping up its campaign against Google’s Chrome browser, using Windows 10 notifications to persuade users to stop using Chrome and switch to its own Edge browser instead.

The software giant in June came out with a blog post that claimed Edge delivers more battery life for users of Windows 10 than Chrome, Firefox and Opera. The notifications, such as this one, appear to be a continuation of that effort.

A Microsoft spokesperson offered this statement Thursday on the notifications:

> "Microsoft Edge was designed exclusively for Windows 10 with features and functionality that enhance the browsing experience such as Cortana, easy sharing, reading and researching. These Windows Tips notifications were created to provide people with quick, easy information that can help them enhance their Windows 10 experience, including information that can help users extend battery life. That said, with Windows 10 you can easily choose the default browser and search engine of your choice."

Still, according to ZDNet, only a quarter of Windows users are using Edge versus competitors, even though the browser is included in Windows 10 by default.

Microsoft once ruled the browser game with Internet Explorer, the predecessor to Edge. Over the last decade, however, it has seen a significant decline in usage as alternatives, especially Chrome and Mozilla’s Firefox, rose to prominence and Internet Explorer failed to keep up with those competitors.

Updated Firefox Is ’Less Susceptible to Freezing’

We’ve all been there. You’re writing an email, scrolling through a website, or watching a video when your browser slows to a crawl, freezes, or fails entirely. It’s a small price to pay for having the Internet at your fingertips, but infuriating nonetheless.

With Firefox 48, Mozilla wants to cut down on these interruptions. The latest version of its browser includes what is known as multi-process dubbed Electrolysis or e10s which is a fancy way of saying Firefox will split up various browser tasks into different processes, so one hiccup won’t derail the entire browsing experience.

"Users should experience a Firefox that is less susceptible to freezing and is generally more responsive to input, while retaining the experiences and features [they] love," product strategist Nick Nguyen wrote in a blog post.

The feature has been in beta for some time, and Mozilla started ramping up for a full release about six weeks ago. Now, E10s will roll out slowly, first to 1 percent of a group of users "that our testing shows it works well for" before expanding to that entire group, which is about half of Firefox 48 users.

To check whether your browser has already enabled e10s, type "about:support" into the URL bar. If the update is active, you’ll see "1/1 (Enabled by default)" next to Multiprocess Windows.

The update also makes "the awesome bar even more awesome," Nguyen said. Now when you enter a query, you’ll see more suggestions in a wider view across the screen. Users can also keep an eye out for more security improvements.

"This is a huge project that will take several more releases to complete, but we’ve got a great foundation in place with the first phase shipping to end users now," Mozilla’s Asa Dotzler and Brad Lassey wrote in a separate blog post. "We’ll build on that foundation to bring even more responsiveness and security to Firefox over the coming months without sacrificing the memory usage advantage we have over our competitors."

Just days after upgrading its iOS app, Mozilla this week enhanced the Firefox for Android app, merging Readings Lists with Bookmarks and Synced tabs with the History Panel, making more content available across all devices. Also look for auto-pause video playback during an incoming phone call and a toolbar to manage audio controls.

What To Expect When The Windows 10 Anniversary Update Installs Itself on Your Computer

Nobody ever accused Microsoft (MSFT) of having consistent naming sequences. Let s see: Windows versions have been named, in order, 1, 2, 3, 95, 98, 2000, ME, XP, Vista, 7, 8 and 10.

And today, there s a new version: Windows 10 Anniversary Update. Why use three syllables when 10 will do?

Windows 10 was already very good. Beautiful, fast, coherent, and compatible with those 4 million Windows apps the world depends on. What Windows 10 AU offers, though, is mostly catchup and refinement. It s a bunch of features that follow in Google s and Apple s footsteps (haters, relax   yes, we know those companies have also stolen from Microsoft), and a lot of fleshing-out of features that were bare-boned in the original Windows 10.

Since Windows 10 AU is free, and since every copy of Windows 10 will soon begin auto-installing the update, you may as well know what you re getting into. Here s a quick rundown of what you have to look forward to.

Edge browser

Microsoft s speedy but stripped-down new web browser, Edge, has finally started to fill in its bald spots. The big news is that it can now accept extensions   feature plug-ins from other companies   just like Firefox, Chrome, and Safari can. There aren t many so far, but the essentials   ad blockers, password memorizers and so on   are already available.

Edge can now pass along notifications (they appear with your other notifications, in the Action Center) from websites that offer them.

You can now pin a tab in Edge (shrink it to an icon that s anchored at the left end of the tab bar), so that you can t close it accidentally.

Finally, Edge uses up a lot less battery power than its rivals, according to Microsoft.

Already, on Microsoft tablets and laptops, you can teach the special camera (an Intel RealSense camera) to recognize you, and log you in with your face. Yes, you can unlock your tablet or laptop just by looking at it   fast, clean, foolproof. (Literally. No photo, sculpture of your head, or even twin can fool this feature.)

That face recognition, along with fingerprint recognition on appropriately equipped laptops, is part of a feature called Windows Hello   and now, Microsoft says, apps and websites can use it, too. Someday soon, you could, in theory, log into your email or bank site just by looking at it.

If it catches on, that will be a huge feature. No more passwords, no more stupid Captcha puzzles to solve. You, and only you, can log in. (Your face or fingerprint is stored only on your machine, and never transmitted.)

If you were kind enough to buy a Microsoft tablet or touchscreen laptop, the company wishes to thank you by bringing you a wagon full of gifts.

You know the pen that came with your recent Surface tablet? You can now program the clicker on the top to do some cool stuff like opening the new Ink Workspace, a collection of pen-friendly apps like Stickies, Sketchpad (for freeform drawing, featuring a virtual ruler you can use as a straightedge), Screen Annotation (lets you draw on a screenshot), and OneNote. (There s a taskbar icon that opens this Workspace, too.)

The new Stickies app recognizes handwritten phone numbers, stock symbols, times, and web addresses (they turn blue once recognized), and offers to dial, look up, create reminders for, or open them when you tap them. That s neat.

The best part of all of this: You can set up the pen-clicker thing to bring up the Ink Workspace even before you ve logged in   at the Lock screen. Finally, a tablet is as useful as a legal pad. You re suddenly getting the phone number of somebody attractive? Click your pen and start writing it down, without first logging in like some kind of painful nerd.(All of this, Microsoft says, may also work with other companies Bluetooth pens.)

Microsoft continues to tinker with the Start menu, the all-knowing oracle that gives you access to everything useful on your PC. Now, the All Programs button is gone; instead, the left side of the Start menu is your All Programs list. (The File, Settings, Power and account buttons are now tiny icons at the even farther left of the menu).

This change makes screaming sense. Every OS includes both a master list of apps and a customizable subset of the ones you use most often   think of the Home screens in Android, or the Dock on the Mac. In Windows 10, the fly-out tiles are your custom subset; the left-hand column should display the master list. You ll fall in love with this feature fast.Too bad you can t type-select an app s name once the list is open, though. (You can type-select only before you ve opened the Start menu, using the Search box.)

Cortana still isn t as smart as Siri or Google Now (here s my comparison). But it s getting steadily better. In AU, you can speak reminders that aren t associated with a particular time or place (Remember that my Delta frequent flyer is   ), and even add photos to them.

Apps and web pages can be programmed to add reminders directly to your list, too. For example, you can save a Map directly into Cortana s reminder list.

Better yet, you can use certain Cortana commands at the lock screen   before you ve even logged in. You can ask her about the news, stocks, or weather, for example, or ask her to tell you a joke. None of this is personal information, so none of it requires signing in.

If you click the clock, you now get a pop-up mini-calendar; click a number to see your appointments for that day. And if you click the volume icon, you can switch playback sources   from speakers to headphones, for example.

 Badges can now appear on app icons, too, just as on the Mac or the iPhone, showing you (for example) how many new messages or emails have come in. Finally, the Action Center (notification list) at the right side has been redesigned it has its own icon to the right of the clock, which sprouts a number to show you how many notifications have piled up   and so has its corresponding Settings screen.

Apple may have introduced the world to the marvels of using your computer to send and receive calls and texts, using your smartphone as a cellular antenna. But in Windows 10 AU, Microsoft has its own version.

The idea is that if you have an Android phone with the Cortana app (or if you re among the six people with Windows phones), all of its notifications and even low-battery alerts can now appear on your Windows desktop, as pop-up alerts. It s pretty crude still in beta   and making it work involves crawling through a bunch of settings on both machines. And, of course, it s not as slick as Apple s; for example, you can t use your laptop or tablet as a speakerphone, as you can on Macs and iPads. But this is a start.

Lots of misc.

Windows 10 AU reserves more slots (10 instead of 5) for ads among your Start-menu tiles (though you can remove them).
Your email address no longer appears on the Lock screen.
You can four-finger swipe between virtual desktops.
You can now use both Microsoft s free antivirus program (Windows Defender) and one that
you ve bought. Defender acts like a second opinion.
New emoji symbols, including bacon and various skin shades.
Lots of the basic starter apps have sprouted new refinements of their own.

Get it?

Windows 10 AU will probably install itself onto your Windows 10 machine this week, or soon; only the subtle Start menu and taskbar changes will alert you that something has changed.

Fortunately, there s very little to dislike in the Anniversary Update. There are very few changes that make you slap your forehead and say, Why did they DO that?!

According to the company, 350 million people are already happily using Windows 10. And with the Anniversary Update, most of them will be even happier.

Microsoft s Giving You Just 10 Days Now, Not 31, To Change Your Mind About Windows 10

Microsoft has hidden a new downgrade policy within the Windows 10 Anniversary Update: Once you ve installed it, you ll only have 10 days to downgrade to an earlier version or build, rather than the 31 days provided before.

Historically, Microsoft had given users a full month to roll back any updates, including upgrades to Windows 10. Supersite for Windows reported this week, however, that it was unable to downgrade to an earlier build after a 10-day limit had expired, though it wasn t exactly clear what builds the limit applied to.

We asked Microsoft for clarification, and it boils down to this: Applying the Anniversary Update triggers the new policy. According to Microsoft, it doesn t matter whether you ve upgraded to Windows 10 from Windows 8 or Windows 7, or whether you simply updated your PC from an earlier version of Windows 10. Once you ve installed the Anniversary Update, you have 10 days to back out, not 31, before the AU becomes permanent.

 T]his new 10-day behavior is for all upgrades and updates to the Anniversary Update, the representative said in an email.

Why this matters: Just when you thought Microsoft s aggressive upgrade practices were over remember all the nastiness about deceptive upgrade tactics? it appears Microsoft is stealthily closing the Windows 10 escape hatch. Recent Windows 10 converts need to figure out when they upgraded to Windows 10, and whether they want to keep it, pronto. And if you upgraded to Windows 10 just so you could downgrade again? You may need to act fast.

I upgraded this PC from Windows 8.1 to Windows 10 on July 28, then upgraded to the Windows 10 AU on Aug. 2. Downgrading back to version 10586 still shows that I have a month (or about Aug. 28) to roll back to Windows 8.1, which is probably still the case.

The problem is that the new rollback period is not clearly defined by Microsoft s own messaging within Windows 10. In fact, it s not defined at all.

In the most recent 14393.10 version of Windows 10 (the Anniversary Update), there’s no time limit attached to the option to go back to a previous build (Settings > Update & Security > Recovery). Even after PCWorld rolled back a second PC on July 28, from the Anniversary Update to the older vanilla version 10586.494, the Settings menu still shows a month remaining. It s also not clear whether rolling back from the AU to version 10586 automatically grants more time.

Microsoft s one-year period to upgrade to Windows 10 from Windows 7 or 8.1, free of charge, ended on July 29. That gave new Windows 10 users just days before the Anniversary Updates began on Aug. 2.

Microsoft isn’t doing this to be mean, though. According to a Microsoft spokesperson, the company’s doing this to free up storage space on your PC. Downloading Windows 10, for example, requires about 3GB of space. Some amount of your drive is also used to store recovery files, whether to recover an upgrade or simply roll back to a previous build.

 Based on our user research, we noticed most users who choose to go back to a previous version of Windows do it within the first several days, Microsoft said in a statement provided to PCWorld. As such, we changed the setting to 10 days to free storage space used by previous copies.

The bottom line is this: If you re an existing Windows 10 user, and not having any issues with the Anniversary Update, you probably don t need to do anything. We consider it to be a positive step forwardfor Windows 10.If you don t like it and want to opt out, including going back to a previous version of Windows, it appears that your new deadline is ten days from August 2, or Friday, August 12.

Does Dropping Malicious USB Sticks Really Work?
Yes, Worryingly Well

Good samaritans and skinflints beware!

Plugging in that USB stick you found lying around on the street outside your office could lead to a security breach.

This is no secret, of course. We have all (hopefully) been aware of the dangers of inserting an unknown USB device into our computers for some time. Heck, the technique has even made it into the Mr Robot TV series.

But what may not be widely known is just how successful the tactic can be for allowing hackers to compromise your computer systems.

Research presented this week at BlackHat by Elie Bursztein of Google s anti-abuse research team shows that the danger is alarmingly real:

we dropped nearly 300 USB sticks on the University of Illinois Urbana-Champaign campus and measured who plugged in the drives. And Oh boy how effective that was! Of the drives we dropped, 98% were picked up and for 45% of the drives, someone not only plugged in the drive but also clicked on files.

It seems folks just can t resist picking up a USB stick that they see lying around Bursztein says that it only took six minutes for the first device that he lost to be picked up.

Bursztein was curious as to whether there were ways of influencing the likelihood of someone plugging a found USB stick into their computer, so they left five different types scattered across the University of Illinois campus: drives labeled exams or confidential , drives with attached keys, drives with keys and a return address label, and generic unlabelled drives.

One would like to imagine that people are less likely to plug in a USB drive if it is clearly labelled with the owner s contact details, and that appears to be borne out by the statistics.

On each type of drive, files consistent with the USB stick s appearance were added. So, private files were added to USB sticks that were unlabelled or were attached to keys or a return label, business files to sticks marked confidential, etc.

However, in reality each of the files was actually an HTML file containing an embedded image hosted on the researcher s server. In this way they were able to track when files were accessed.

Upon opening the HTML file, users were asked if they wished to participate in a survey asking why they plugged in the drive. Approximately 20% agreed (perhaps encouraged by the promise of a gift card for their assistance).

Just over two thirds of the people who responded to the survey said that they accessed the USB sticks with the intention of returning them to their rightful owner. 18% admitted that they were curious , and 14% gave other explanations.

Now from the security point of view it s worth recognising that a security breach could already have happened by this point.

The most basic   and simplest to conduct   attack would have seen malicious code placed in the HTML file that would have been automatically activated upon viewing, perhaps downloading further malware from the internet. Alternatively, users could have been taken to a phishing site, and tricked into handing over login credentials through social engineering.

In addition, there is also always the danger that an attacker might have planted executable malware directly onto the USB stick, and hoped that an unsuspecting user would allow it to run on their computer.

A more sophisticated attack, however, would see the use of a device using HID (Human Interface Device) spoofing to trick a computer into believing that it was in reality a keyboard. As soon as the USB stick is plugged in it would inject keystrokes   building a set of commands that could open a reverse shell that could give a hacker remote access to the victim s computer.

In a blog post, Bursztein explains in depth how he was able to camouflage a keyboard-spoofing device so that it looked near-identical to a genuine USB stick.

Keyboard-spoofing is not the most sophisticated type of attack possible through a malicious USB stick however.

Perhaps the most complex and stealthy attack would see the plugged-in device exploiting a zero-day vulnerability in the computer s USB driver   similar to the method used in the notorious Stuxnet attack against the Natanz uranium enrichment facility in Iran.

Your chances of having a USB zero-day vulnerability used against your organisation is remote, unless you are of particular interest to an intelligence agency or state-sponsored hackers.

Keyboard-spoofing HID attacks and especially basic social engineering attacks tricking users into opening files on a newly-found USB stick, however, are much more likely, which means it is essential that you educate your workers about the risks and urge them to hand lost property in rather than attempting to identify a device s owner themselves.

In short:

USB devices should be treated with caution. Never plug in an unattended, unidentified USB stick.

Keep your security defences, policies and patches up to date.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.